

## 明 細 書

## 量子暗号通信装置

## 5 技術分野

この発明は、位相変調方式の量子暗号において、送信者側で量子を秘密情報で変調した後伝送し、受信者側で受信した量子を復調することで秘密情報を共有する量子暗号通信装置に関するものである。

## 10 背景技術

量子暗号通信とは、送信者側が量子、一般的には光子を秘密情報で変調した後伝送し、受信者側が受信した量子を復調することで秘密情報を共有する通信方式である。量子に載せられた秘密情報は量子力学の不確定性原理により安全性が保証されている。但し、量子は壊れやすく、全ての情報を確実に伝送できるわけではないため、秘密情報としては乱数情報を用いている。送受信者間で伝送される乱数情報は、誤り訂正や守秘性を高める等のデータ処理を行った後、暗号通信用の秘密鍵として用いられる。これを特に量子鍵配布と呼んでいる。

ところで、位相変調方式は、光ファイバ通信をベースにした量子暗号において好適に用いられる変調方式である。これは、信号光パルスと参照光パルスという時間差2連光子パルスの相対位相情報が光ファイバ伝送中に比較的良好に保存されるためである。相対位相情報は、信号光パルスと参照光パルスとを合波した際に生じる干渉現象を観測することで復調できる。このため、位相変調方式の量子暗号通信装置では、送信装置側に2連光子パルスを発生させるための非対称マッハツェンダ干渉計と呼ばれるループ状光路を持ち、受信装置側に2連光子パルスを合波、干渉させるための同じ大きさの非対称マッハツェンダ干渉計を持つ構成が一般的である。

しかしながら、このような構成の量子暗号通信装置においては、以下の2つの揺らぎの効果が無視できない影響を及ぼしている。1つは、通信路の持つ複屈折性の偏波揺らぎであり、もう1つは、送受信装置が持つ2つの非対称マッハツェ

ンダ干渉計の間に生じる光路長揺らぎである。この2つの揺らぎのため、上記構成の量子暗号通信装置では絶え間ない偏波および光路長の調整が必要であった。

これに対して、デファクト化が進行している。プラグ&プレイ方式と呼ばれる量子暗号通信装置は、量子受信装置から量子送信装置へ、量子送信装置から量子受信装置へと2連光子パルスを送り、量子送信装置内で非相対的に各光パルスの偏波面を直角に回転させた後反射することで、量子伝送路上で被る偏波揺らぎを往路と復路とで相殺し、偏波揺らぎの自動補償を実現している。また、量子受信装置内で信号光と参照光という時間差のある2連光子パルスを発生させるためのループ状光路と2連光子パルスを合波、干渉させるためのループ状光路とを同一にすることで、光路長揺らぎの補償された安定な合波、干渉を実現していた（例えば、特許文献1及び3、非特許文献1参照）。

なお、上記のようなプラグ&プレイ方式の量子暗号通信装置において、特に量子送信装置を構成する光学系の1構成例として、量子暗号に特化した光学系ではないが、偏波回転ミラーを用いた光学系の構成も可能である（例えば、特許文献2参照）。

特許文献1：特開2002-289298号公報（段落0033、図1）

特許文献2：特開平5-241104号公報（段落0012、図4（a）、図5（b））

特許文献3：US 6, 188, 768 B1（図2、図4及び第6頁）

20 非特許文献1：G. Ribordy, et. al. "Automated "Plug & Play" Quantum Key Distribution" Electronics Letters 34, (22), pp. 2116-2117, 1998

従来のプラグ&プレイ方式の量子暗号通信装置は、光子パルスが同一光路上を往復することで揺らぎに対して安定な系を構成しているが、このために、光子パルスが量子受信装置内の位相変調器を往路と復路とで2回通過しなければならない。通信速度を高速にするために光源の繰り返し周波数を上げていき、光子パルスが光路を往復するのにかかる時間よりも短い周期で光子パルスが発振されるようになると、1周期の中での往路光子パルスが位相変調器を通過するタイミングと復路光子パルスが位相変調器を通過するタイミングが接近し、選択した繰り返し周波数によっては復路光子パルスの方に位相変調をかけるつもりでも、位相変

調不要な往路光子パルスにも位相変調がかかってしまうという問題点があった。

この発明は上記のような問題点を解決するためになされたもので、往路光子パルスに位相変調がかかることを防ぎ、通信速度高速化のために光源の繰り返し周波数を自由に選択できる量子暗号通信装置を得ることを目的とする。

5

#### 発明の開示

この発明に係る量子暗号通信装置は、量子を伝送するための量子通信路と、前記量子伝送路の送信側に設置された量子送信装置と、前記量子伝送路の受信側に設置された量子受信装置と、前記量子送信装置と前記量子受信装置を結合して同期信号を含む制御信号を相互通信するための制御信号通信路とを備えた量子暗号通信装置であって、前記量子受信装置は、量子源となる光源と、前記光源から出た光子パルスから信号光パルスと参照光パルスとの時間差 2 連光子パルスを発生すると共に、逆進する量子である信号光パルスと参照光パルスとを合波、干渉させるための合波干渉手段を有するループ状光路と、前記量子通信路との接続口に設けられて、前記時間差 2 連光子パルスが前記量子通信路を介して前記量子送信装置と前記量子受信装置との間を往復した後、受信される前記参照光パルスのみに対して位相変調をかける位相変調器を有する迂回光路と、前記ループ状光路を介した干渉光を観測する光子検出器とを含み、前記量子送信装置は、前記量子受信装置から前記量子通信路を介して到達した 2 連光子パルスの偏波面を非相対的に直角に回転させる偏波回転手段と、前記偏波回転手段を通過した信号光パルスに位相変調をかけて再び量子通信路を通して前記量子受信装置に戻す位相変調器と、信号光パルスをパルス中に光子が 2 個以上含まない状態まで減光する減光手段とを含むことを特徴とする。

25

#### 図面の簡単な説明

図 1 は、この発明の実施の形態 1 に係る量子暗号通信装置を示す構成図、

図 2 A は、図 1 に示す非対称マッハツェンダ干渉計と位相変調器用迂回光路の構成図、

図 2 B は、図 2 A の位相変調器用迂回光路の変形構成図、

- 図 2 C は、図 2 A の非対称マッハツェンダ干渉計の変形構成図、  
図 2 D は、図 2 A の非対称マッハツェンダ干渉計の変形構成図、  
図 3 A は、図 1 に示す量子送信装置の光学系の構成図、  
図 3 B は、図 1 に示す量子送信装置の光学系の変形構成図、  
5 図 3 C は、図 1 に示す量子送信装置の光学系の変形構成図、  
図 3 D は、図 1 に示す量子送信装置の光学系の変形構成図、  
図 3 E は、図 1 に示す量子送信装置の光学系の変形構成図、  
図 4 は、図 1 に示すこの発明の実施の形態 1 による量子通信動作を説明するフローチャート、  
10 図 5 は、この発明の実施の形態 2 に係る量子暗号通信装置を示す構成図、  
図 6 A は、図 5 に示す量子受信装置の光学系の構成図、  
図 6 B は、図 5 に示す量子受信装置の光学系の変形構成図、  
図 6 C は、図 5 に示す量子受信装置の光学系の変形構成図、  
図 6 D は、図 5 に示す量子受信装置の光学系の変形構成図、  
15 図 6 E は、図 5 に示す量子受信装置の光学系の変形構成図、  
図 7 は、図 5 に示すこの発明の実施の形態 2 による量子通信動作を説明するフローチャートである。

#### 発明を実施するための最良の形態

##### 20 実施の形態 1.

図 1 は、この発明の実施の形態 1 に係る量子暗号通信装置を示す構成図であり、光ファイバに基づく位相変調方式を用いた装置の全体構成を示している。

- 図 1 に示す量子暗号通信装置は、送信側の量子送信装置 100 と、受信側の量子受信装置 200 と、量子送信装置 100 および量子受信装置 200 を相互接続するための量子伝送路となる光ファイバ通信路 1 と、公開通信路 2 および制御信号通信路 3 とにより構成されている。
- 25

量子送信装置 100 および量子受信装置 200 は、量子として振舞う光子を伝送する光ファイバ通信路 1 と、LAN やインターネットで代表される公開通信路 2 と、制御信号通信路 3 とを介して相互に接続される。

光ファイバ通信路 1 は、量子暗号を含む量子信号を伝送し、制御信号通信路 3 は、量子送信装置 100 および量子受信装置 200 を同期・調歩動作させるための制御信号を伝送する。また、制御信号通信路 3 としては、具体的には、光ファイバ通信路 1 または公開通信路 2 が用いられてもよい。

- 5 量子送信装置 100 は、前述した特許文献 2 に記載された光学系と類似の構成を有しており、光ファイバ通信路 1 に一端が接続されたアッテネータ 14 と、アッテネータ 14 の他端の光路に接続された偏光ビームスプリッタ 15 と、偏光ビームスプリッタ 15 の 2 つの光路に個別に接続されたファラデー回転子 16 および位相変調器 17 と、位相変調器 17 を制御する送信側制御手段 20 と、送信側制御手段 20 に接続されて第 1 の乱数を出力する送信側データ処理手段 22 と
- 10 側制御手段 20 に接続されて第 1 の乱数を出力する送信側データ処理手段 22 とを備えている。

- 偏光ビームスプリッタ 15、ファラデー回転子 16 および位相変調器 17 は、量子通信用の光子パルスに対する両回転方向の光路ループを構成しており、量子送信装置 100 は、量子受信装置 200 から導入された光子パルスを、光ファイバ通信路 1 およびアッテネータ 14 を介してファラデー回転子 16 に導入し、非相反的に偏波面を直角に回転させる偏波回転手段としてのファラデー回転子（非相反素子） 16 を通した後、再度アッテネータ 14 および光ファイバ通信路 1 を介して量子受信装置 200 に向けて反射して戻すようになっている。なお、アッテネータ 14 は、信号光パルスをパルス中に光子が 2 個以上含まない状態
- 15 まで減光する減光手段をなす。

- 一方、量子受信装置 200 は、量子源となる光子を発生する光源としての光子発生器 4 と、光子発生器 4 の出力光路に一端が接続された偏光子 5 と、偏光子 5 の他端に P 偏光出力ポートが接続された偏光ビームスプリッタ 6 と、偏光ビームスプリッタ 6 の S 偏光出力ポートに接続された光子検出器 19 と、偏光ビームスプリッタ 6 の合波光入力ポートに配設されたビームスプリッタ 7、8 およびミラー 9、10 からなる非対称マッハツェンダ干渉計と、非対称マッハツェンダ干渉計のビームスプリッタ 7 の残った出力ポートに接続された光子検出器 18 と、非対称マッハツェンダ干渉計のビームスプリッタ 8 の出力ポートに合波光入力ポートが接続された偏光ビームスプリッタ 11 と、偏光ビームスプリッタ 11 の S 偏
- 20
- 25

光出力ポートに接続された位相変調器 13 と、偏光ビームスプリッタ 11 の P 偏光出力ポートに P 偏光出力ポートが接続され、かつ、位相変調器 13 の他端が S 偏光出力ポートに接続され、かつ、合波光入力ポートが光ファイバ通信路 1 に接続された偏光ビームスプリッタ 12 と、光子検出器 18、19 の検出信号を取り込み、かつ、位相変調器 13 と光子検出器 18、19 と光子発生器 4 を制御する受信側制御手段 21 と、受信側制御手段 21 に接続されて第 2 の乱数を出し、光子検出信号を入力する受信側データ処理手段 23 とを備えている。

量子受信装置 200 内の偏光ビームスプリッタ 12 は、光ファイバ通信路 1 を介して量子送信装置 100 内のアッテネータ 14 に接続され、受信側制御手段 21 は、制御信号通信路 3 を介して送信側制御手段 20 に接続され、受信側データ処理手段 23 は、公開通信路 2 を介して送信側データ処理手段 22 に接続されている。

量子受信装置 200 内において、ビームスプリッタ 7、8 およびミラー 9、10 からなる非対称マッハツェンダ干渉計は、光子発生器 4 から発生した光子パルスを信号光パルスと参照光パルスとの時間差 2 連光子パルスに分離するループ状光路を形成し、ここで、ビームスプリッタ 7 は、逆進する量子である信号光パルスと参照光パルスとの合波、干渉を引き起こす合波干渉手段として機能する。

また、量子受信装置 200 内において、偏光ビームスプリッタ 11、12 は、2 つの直交する偏波モードを分離し、P 偏光した光子が量子受信装置 200 から量子送信装置 100 へ伝送する際には、偏光ビームスプリッタ 11、12 を短絡する光路が選択され、S 偏光した光子が量子送信装置 100 から量子受信装置 200 へ伝送する際には、位相変調器 13 を経由する迂回光路が選択される。

次に、図 1 に示したこの発明の実施の形態 1 に係る量子暗号通信装置の動作について説明する。

受信側制御手段 21 は、制御信号通信路 3 を介した制御信号の相互通信により、量子送信装置 100 内の送信側制御手段 20 と同期・調歩動作する。

量子受信装置 200 内の光子発生器 4 は、受信側制御手段 21 が出力する同期信号に応じて偏波面の揃った光子パルスを発生する。

光子発生器 4 から発生した光子パルスは、偏光ビームスプリッタ 6 の P 偏光に

あたる偏波面のみが通過するように設置されている偏光子 5 によって、偏波面が整えられた後、非対称マッハツェンダ干渉計に入光する。非対称マッハツェンダ干渉計に入光した光子パルスは、偏波面の揃った可干渉な時間差を有する参照光パルスと信号光パルスと呼ばれる 2 連光子パルスに分離され、偏光ビームスプリッタ 11 に導かれる。

ここで、2 連光子パルスのうち先行する第 1 の光子パルス（参照光パルス）は、ビームスプリッタ 7 から直にビームスプリッタ 8 へ進行した光子パルスであり、他方の後続する第 2 の光子パルス（信号光パルス）はビームスプリッタ 7 で反射されてミラー 9、10 を通過する光子パルスである。偏光ビームスプリッタ 11 に導かれた 2 連光子パルスは、偏光ビームスプリッタ 6 と同じに偏光面が設定されている偏光ビームスプリッタ 11、12 をこの順に通過し、位相変調器 13 のある迂回光路に導かれることなく、光ファイバ通信路 1 に導かれる。

なお、図 1 における非対称マッハツェンダ干渉計と位相変調器用迂回光路の構成例としては種々採用できる。図 2 A は、図 1 に示す非対称マッハツェンダ干渉計の構成例であり、ビームスプリッタ 7、8 とミラー 9、10 とを用い、位相変調器用迂回光路の構成例として、 $1 \times 2$ （1 入力 2 出力または 2 入力 1 出力）タイプの偏光ビームスプリッタ 11、12 とで 2 式を用いた構成例を示したが、図 2 B に示すように、 $2 \times 2$ （2 入力 2 出力または 2 入力 2 出力）タイプの偏光ビームスプリッタ 24 を 1 式用いた迂回光路の構成例や、図 2 C に示すように、カプラ 25、26 と遅延ファイバ 27 を用いた非対称マッハツェンダ干渉計の構成例や、図 2 D に示すように、カプラ 28 とファラデーミラー 29、30 を用いた非対称マッハツェンダ干渉計の構成例も存在し、特定の 1 つの構成例に特化されるものではない。なお、図 2 D において、31 はサーキュレータを示す。

量子受信装置 200 から光ファイバ通信路 1 に導かれた 2 連光子パルスは、量子送信装置 100 に導入され、量子送信装置 100 内のファラデー回転子 16 により偏波面を非相反的に直角に回転させられ、位相変調器 17 により信号光パルスが位相変調を受けた後、再び量子受信装置 200 に帰還してくる。

なお、図 1 における量子送信装置の光学系の構成例としては種々採用できる。図 3 A は、図 1 に示す量子送信装置の光学系の構成例であり、アッテネータ 14

- と偏光ビームスプリッタ 15 とファラデー回転子 16 と位相変調器 17 を用いた構成例を示したが、図 3 B に示すように、2 個の 1 × 2 偏光ビームスプリッタ 32, 33、2 個の位相変調器 34, 35 およびファラデーミラー 36 を用いた構成例や、図 3 C に示すように、2 個の 1 × 2 偏光ビームスプリッタ 37, 38、位相変調器 39 およびファラデーミラー 40 を用いた構成例や、図 3 D に示すように、2 × 2 偏光ビームスプリッタ 41、位相変調器 42 およびファラデーミラー 43 を用いた構成例や、図 3 E に示すように、偏波無依存の位相変調器 44 およびファラデーミラー 45 を用いた構成例も存在し、1 つの構成例に特化されるものではない。
- 10 量子受信装置 200 に帰還した 2 連光子パルスは、偏光ビームスプリッタ 12 で完全に反射されて、位相変調器 13 が配置された迂回光路に導かれる。なぜならば、光ファイバ通信路 1 の一方の端点で入射された光が他方の端点で非相反的に直角に偏波面の回転を受けて反射して帰還する場合に、途中の光路でいかなる複屈折性の揺らぎが存在したとしても、入射した時点から直角に偏波面が回転した状態で帰還するからである。
- 15 偏光ビームスプリッタ 12 で反射された 2 連光子パルスは、位相変調器 13 に入光する。このとき、位相変調器 13 は、受信側制御手段 21 の制御下で、受信側データ処理手段 23 が出力した第 2 の乱数に応じて、参照光パルスのみに対して位相変調をかける。
- 20 位相変調器 13 を通過した 2 連光子パルスは、偏光ビームスプリッタ 11 で完全に反射されて非対称マッハツェンダ干渉計へと導かれる。このとき、非対称マッハツェンダ干渉計は、先行する参照光パルスを時間差の有する参照光 2 連光子パルス、すなわち、ビームスプリッタ 8 からビームスプリッタ 7 に直行する参照光の先行光子パルスと、ミラー 10、9 を通過する参照光の後続光子パルスに分割し、同様に後続する信号光パルスを、時間差の有する信号光 2 連光子パルス、すなわち、ビームスプリッタ 8 からビームスプリッタ 7 に直行する信号光の先行光子パルスと、ミラー 10、9 を通過する信号光の後続光子パルスに分割する。
- 25 ここで、非対称マッハツェンダ干渉計で往路、復路ともに同じ光路を用いているので、各 2 連光子パルスの各時間差は自動的に全く同じとなる。



従って、参照光の後続光子パルスと信号光の先行光子パルスは同時にビームスプリッタ 7 に到達して干渉を引き起こすことになる。干渉を引き起こした光子パルスは、排他的に 1 対の光子検出器 18、19 のいずれかに接続する一方のポートに導かれ、一方の光子検出器を発火する。なお、光子検出器 19 に接続するポ  
5      ートに導かれた光子パルスは、偏光ビームスプリッタ 6 により完全に反射されて、光子検出器 19 に導かれることになる。

受信側制御手段 21 は、光子検出器 18、19 のいずれが発火したかをビット情報に変換し、受信側データ処理手段 23 に伝送する。受信側データ処理手段 23 は、第 2 の乱数と、量子情報で伝送されたビット情報とから、公開通信路 2 を  
10      用いて、量子送信装置 100 と情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、量子送信装置 100 に注目しながら、具体的な動作について説明する。

量子受信装置 200 から光ファイバ通信路 1 を通過して量子送信装置 100 に導入された 2 連光子パルスは、量子送信装置 100 に到達した時点では、光ファイバ通信路 1 の有する複屈折性の揺らぎにより偏波面が完全にランダムな状態に  
15      なっている。この状態で、量子送信装置 100 に導入された 2 連光子パルスは、アッテネータ 14 で減衰された後、偏光ビームスプリッタ 15 によりそれぞれ直交する 2 つの偏波モード（P 偏光と S 偏光）に分離される。

このようにして、4 つに分離された光子パルスのうち、時計回りに進行する 2  
20      連光子パルス（S 偏光）は、偏光ビームスプリッタ 15 で反射され、位相変調器 17 を通過した後、ファラデー回転子 16 で非相反的に偏波面を直角に回転させられた後、偏光ビームスプリッタ 15 に戻る。

また、4 つに分離された光子パルスのうち、反時計回りに進行する 2 連光子パルス（P 偏光）は、偏光ビームスプリッタ 15 を通過し、ファラデー回転子 1  
25      6 で非相反的に偏波面を直角に回転させられて、位相変調器 17 を通過した後、偏光ビームスプリッタ 15 に戻る。

このとき、位相変調器 17 は、送信側制御手段 20 の制御下で、送信側制御手段 22 が出力した第 1 の乱数に応じて、2 連光子パルスのうち信号光パルスのみに対して、時計回りまたは反時計回りの進行方向に依存することなく、位相変調

器 1 7 を通過する際に位相変調をかけている。

偏光ビームスプリッタ 1 5 に戻った 4 つの光子パルスは分離合流するまでの光路長が、時計回りまたは反時計回りに依存せずに等しいので、再び 2 連光子パルスとなり、アッテネータ 1 4 に導入される。

- 5      ここで、アッテネータ 1 4 の光子レベル強度の減衰の大きさは、信号光パルスの光子数が「1」を越えない強度となるように調整されている。

このようにして、再び光ファイバ通信路 1 に導入されて量子受信装置 2 0 0 に帰還した 2 連光子パルスは、前述したとおり、偏光ビームスプリッタ 1 2 により完全に反射されて、位相変調器 1 3 のある迂回光路を通った後、偏光ビームスプリッタ 1 1 で反射されて、光子検出器 1 8、1 9 の設置されたポートに導かれる。

以下、受信側制御手段 2 1 は、光子検出器 1 8、1 9 のいずれが発火したかをビット情報に変換して受信側データ処理手段 2 3 に伝送する。

- 15      上記の 1 パルス当たりの量子通信を、あらかじめ定めた回数だけ繰り返した後、送信側データ処理手段 2 2 および受信側データ処理手段 2 3 は、量子伝送路（光ファイバ通信路 1）を介して秘匿性を保って伝送された情報と、公開通信路 2 を介して伝送された情報とを用いて秘匿性情報を共有する。すなわち、第 1 および第 2 の乱数と、量子通信で伝送されたビット情報とから、公開通信路 2 を用いて、情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

- 20      次に、図 4 に示すフローチャートを参照しながら、図 1 に示したこの発明の実施の形態 1 による量子通信動作について、さらに具体的に説明する。

- 25      図 4 において、量子暗号通信装置の光子パルス（量子暗号）に関連した量子通信部の処理ステップは、光子発生ステップ S 1 と、光パルス分離・合流ステップ S 2 と、位相変調器 1 3 を経由しない光路を選択する光路選択ステップ S 3 と、量子受信装置 2 0 0 から量子送信装置 1 0 0 への量子通信用の光子供給（往路）ステップ S 4 と、送信側での第 1 アッテネートステップ S 5 と、第 1 ファラデー回転ステップ S 6 と、第 1 送信側位相変調ステップ S 7 と、第 2 受信側位相変調ステップ S 6 a と、第 2 ファラデー回転ステップ S 7 a と、第 2 アッテネートステップ S 8 と、量子送信装置 1 0 0 から量子受信装置 2 0 0 への量子通信用

の光子伝送（復路）ステップS 9と、受信側位相変調ステップS 10と、光子分離・合流・干渉ステップS 11と、光子検出ステップS 12とを含む。

まず、量子受信装置200内の光子発生器4は、受信側制御手段21の制御下で光子パルスが発生する。発生した光子パルスは、偏光子5により偏光ビームスプリッタ6のP偏光に相当する光子パルスのみが通過する。P偏光に偏波面が揃えられた光子パルスは、偏光ビームスプリッタ6を透過する（光子発生ステップS 1）。なお、光子パルスは、例えばレーザーパルスのように、パルス当たりの光子数がポアソン分布に従うように発生されてもよく、単一光子源を用いて、パルス当たり単一光子として発生されてもよい。

- 10 偏光ビームスプリッタ6を透過した光子パルスは、ビームスプリッタ7、8およびミラー9、10により構成される非対称マッハツェンダ干渉計に導かれる。非対称マッハツェンダ干渉計に導かれた光子パルスは、この非対称マッハツェンダ干渉計内において光路長の異なる2つの光路に分離された後、再度合流して出力されることにより、光路長に応じた時間差を有する2連光子パルスとなる（光
- 15 パルス分離・合流ステップS 2）。なお、この非対称マッハツェンダ干渉計内では偏波面が保持される構成となっている。

- 非対称マッハツェンダ干渉計から出力された2連光子パルスは、先行する参照光パルスと後続する信号光パルスとにより構成され、いずれの光子パルスも偏波面が偏光ビームスプリッタ11、12に対してP偏光となるように偏波面が揃っている
- 20 ているので、偏光ビームスプリッタ11および12を透過する光路が選択される（光路選択ステップS 3）。

- 偏光ビームスプリッタ12を透過した2連光子パルスは、光ファイバ通信路1に導かれ、そのまま量子送信装置100に伝送される（光子供給（往路）ステップS 4）。このとき、光ファイバ通信路1が有する複屈折性の揺らぎにより、2
- 25 連光子パルスの偏波面は完全にランダムな状態になってしまう。

量子送信装置100に導かれた2連光子パルスは、アッテネータ14を透過することによって、パルス当たりの光子数が減衰された後、偏光ビームスプリッタ15に導かれる（第1アッテネートステップS 5）。

また、量子送信装置100に導入された2連光子パルスは、各偏波面がランダ

ムなので、偏光ビームスプリッタ 15 において、時計回りで周回する光子パルスと反時計回りで周回する光子パルスとに分離された後、再び偏光ビームスプリッタ 15 で合流して 2 連光子パルスに戻る。

- すなわち、2 連光子パルスのうちの反時計回りの光子パルスは、光路ループ内  
5 において、ファラデー回転子 16 および位相変調器 17 の順に通過し、ファラデー回転子 16 を通るときに、偏波面が非相反的に直角に回転させられる（第 1 ファラデー回転ステップ S 6）

- また、反時計回りの光子パルスは、ファラデー回転子 16 を通過した後、位相変調器 17 に導入され、位相変調器 17 を通過する際に、信号光パルスに当たる光子パルスのみが位相変調を受ける（第 1 送信側位相変調ステップ S 7）。

このときの位相変調の大きさは、送信側制御手段 20 により制御され、送信側データ処理手段 22 が出力した第 1 の乱数に応じて、制御信号通信路 3 を介して、同期タイミングを調整しつつ位相変調をかけることによって決定される。

- 一方、量子送信装置 100 に導入された 2 連光子パルスのうち、時計回りの光子パルス  
15 の場合は、光路ループ内において、位相変調器 17 およびファラデー回転子 16 の順に通過するので、先に第 2 送信側位相変調ステップ S 6 a を経た後に、第 2 ファラデー回転ステップ S 7 a が実行される。なお、ファラデー回転子（非相反素子）16 による非相反的な偏波面の回転とは、回転の向きが光子パルスの進行方向に依存しないことを意味する。

- 20 また、光路ループ内の位相変調器 17 において、反時計回りの光子パルスおよび時計回りの光子パルスのいずれに対しても、信号光パルスのみに対して選択的に位相変調をかけるためには、偏光ビームスプリッタ 15、ファラデー回転子 16 および位相変調器 17 を含む光路ループの光路長を、入射される 2 連光子パルスの時間差に相当する距離に比べて十分に短く設定すればよく、容易に実現  
25 することができる。

偏光ビームスプリッタ 15 を介して、再び 2 連光子パルスに戻った光子パルスは、アッテネータ 14 を再度通過する。このとき、信号光パルスの光子数が「1」を越えない程度まで、パルス当たりの光子レベル強度が減衰された後、光ファイバ通信路 1 に導入される（第 2 アッテネートステップ S 8）。

光ファイバ通信路 1 に再入射した 2 連光子パルスは、量子受信装置 200 に向かって帰還することになるが、このとき、2 連光子パルスの偏波状態は、光ファイバ通信路 1 の有する複屈折性の揺らぎによって、再びランダムな変動を受ける。

- 5       しかし、光ファイバ通信路 1 に再入射した 2 連光子パルスの偏波面は、量子送信装置 100 内のファラデー回転子 16 により、非相反的に直角に回転を受けているので、光ファイバ通信路 1 の往路上で受けた偏波変動と、復路上で受けた偏波変動が丁度打ち消し合うように作用する。

- 従って、再導入された 2 連光子パルスが量子受信装置 200 内の偏光ビームスプリッタ 12 に到達する時点では、2 連光子パルスの偏波面は、偏光ビームスプリッタ 12 から量子送信装置 100 に向かった往路時と比べて、正確に直角に回転している（光子伝送（復路）ステップ S 9）。

- このように、量子受信装置 200 に到達した 2 連光子パルスは、偏波面が直角に回転した、偏光ビームスプリッタ 12 にとって S 偏光にあたる偏波面でもって、偏光ビームスプリッタ 12 に導かれるので、偏光ビームスプリッタ 12 において完全に反射され、位相変調器 13 のある迂回光路に導かれる。2 連光子パルスが位相変調器 13 を通過する際に、参照光パルスのみが位相変調を受ける（受信側位相変調ステップ S 10）。このときの位相変調の大きさは、受信側制御手段 21 により制御され、受信側データ処理手段 23 が出力した第 2 の乱数に応じて、位相変調の大きさが決定される。

2 連光子パルスは位相変調器 13 を通過後、偏光ビームスプリッタ 11 で完全に反射されて、ビームスプリッタ 8、7 およびミラー 10、9 により構成される往路で通過した非対称マッハツェンダ干渉計に再度導かれる。

- 非対称マッハツェンダ干渉計に再導入された 2 連光子パルスは、前述と同様に、それぞれ光路長の異なる 2 つの光路に分離された後、再度合流するまで、4 つの光子パルスに分かれることになる。

すなわち、非対称マッハツェンダ干渉計に導入された 2 連光子パルスのうち、参照光パルスは、ビームスプリッタ 8 からビームスプリッタ 7 に直行する参照光先行光子パルスと、ミラー 10、9 を通過する参照光後続光子パルスとに分離さ

れる。

同様に、信号光パルスは、ビームスプリッタ 8 からビームスプリッタ 7 に直行する信号光先行光子パルスと、ミラー 10、9 を通過する信号光後続光子パルスとに分離される。

- 5      上記 4 つの光子パルスは、ビームスプリッタ 7 で再び合流するが、光路長差により時間差が生じている。

但し、往路で通過した非対称マッハツェンダ干渉計を復路で再び通過するため、時間差が自動的に完全に一致する参照光後続光子パルスと信号光先行光子パルスは、ビームスプリッタ 7 に同時に到達し、干渉を引き起こすことになる（光子

- 10    分離・合流・干渉ステップ S 11）。

ビームスプリッタ 7 における干渉の結果、参照光後続光子パルスおよび信号光先行光子パルスの合流光子パルスは、光子検出器 18 または 19 のいずれかの一方に排他的に導かれることになる。

- 15    なお、光子検出器 19 のある光路に導かれた光子パルスは、偏波面が往路のときと比べて直角に回転しているので、偏光ビームスプリッタ 6 で完全に反射されて、光子検出器 19 に導かれる。

- 合流光子パルスが光子検出器 18、19 のどちらかに導かれるかは、第 1 送信側位相変調ステップ S 7 において信号光パルスが受けた位相変調と、受信側位相変調ステップ S 10 において参照光パルスが受けた位相変調との位相差により確率的に決定される。但し、上記位相差が「0」または「 $\pi$ 」の場合には、合流光子パルスの導かれる光子検出器が確定する。
- 20

このようにして、光子検出器 18、19 には、参照光先行光子パルスと、合流光子パルス（参照光後続光子パルスおよび信号光先行光子パルス）と、信号光後続光子パルスとがそれぞれ導かれる。

- 25    ここで、タイミングを調整することにより、合流光子パルスが導かれたときのみに、光子検出器 18、19 の一方を発火させることができる。

または、光子検出器 18、19 のいずれが発火してもよいが、受信側制御手段 21 により、合流光子パルスが導かれたタイミングの発火のみを有効とすることができる。

いずれにせよ、受信側制御手段 21 は、光子検出器 18、19 のどちらかが発火したことにより、「0」または「1」の量子通信ビット情報を定め、この量子通信ビット情報を受信側データ処理手段 23 に送る（光子検出ステップ S12）。

5      以上が量子通信部の光子パルス当たりの動作フローである。

上記量子通信動作は、予め定めた回数だけ繰り返し実行され、その後、送信側データ処理手段 22 および受信側データ処理手段 23 は、公開通信路 2 を用いて相互に情報交換をしつつ、第 1 および第 2 の乱数と量子通信ビット情報から、秘匿性が保証されたランダムな情報を共有する。

10      このように、量子受信装置 200 内において、非対称マッハツェンダ干渉計から出力されて、再び、同一の非対称マッハツェンダ干渉計に導入される光子パルスは、光ファイバ通信路 1 の有する任意の複屈折性揺らぎに起因してランダムな偏波変動が生じて、光ファイバ通信路 1 の送信側端（量子送信装置 100 内のファラデー回転子 16）で非相対的に直角に偏波面が回転されて往復すること  
15      により、ランダムな偏波変動が打ち消されることになる。

従って、非対称マッハツェンダ干渉計に再導入された光子パルスは、偏波面が自動的に完全に整えられているので、偏波無依存性が要求されることは全くなく、偏波依存性を有していたとしても、光子パルスの偏波面の調整が全く不要となる。

20      また、往路において光子パルスを 2 連光子パルスに分離するために用いた非対称マッハツェンダ干渉計と、復路において、2 連光子パルスを合流・干渉させるために用いた非対称マッハツェンダ干渉計に同一のものをを用いているため、光路長差の調整が全く不要であり、かつ、光路長揺らぎに対しても自動的に補償されるような構成となり、安定な干渉系を構成することができる。

25      また、量子受信装置 200 内の光路において、位相変調器 13 を通る迂回光路を設け、上記のような量子送信装置 100 内で偏波面が直角に回転されることを利用して、量子受信装置 200 内で、光子発生器 4 から光ファイバ通信路 1 に向かう往路においては、光子パルスが位相変調器 13 の無い光路を自動的に選択し、光ファイバ通信路 1 から光子検出器 18、19 に向かう復路においては、光子

パルスが位相変調器 13 のある迂回光路を自動的に選択するようにしたことで、位相変調器 13 において光子パルスの流れは一方向に限定され、光子パルスに不適切な位相変調がかけられるおそれが全くなり、光子パルス発生 of 繰り返し周波数を自由に選択することができる。

5

実施の形態 2.

上述した実施の形態 1 では、2 連光子パルスの偏波面が揃っているため、偏光ビームスプリッタ 11、12 のみで位相変調器 13 を配置する迂回光路を実現したが、この実施の形態 2 では、特許文献 1 及び 3、非特許文献 1 に記載された光学系のように、2 連光子パルスの偏波面が揃っていない場合に、偏光ビームスプリッタと偏光変調器を用いて、位相変調器を配置した迂回光路を実現する場合を示す。

図 5 は、量子受信装置 200 内に偏光変調器 9 を設けたこの発明の実施の形態 2 に係る量子暗号通信装置を示す構成図である。図 5 において、量子送信装置 100 は、特許文献 3 に記載された光学系と類似の構成を有しており、光ファイバ通信路 1 に一端が接続されたアッテネータ 14 と、アッテネータ 14 の他端の光路に接続された偏光ビームスプリッタ 15 と、偏光ビームスプリッタ 15 の P 偏光出力ポートに接続された偏光ビームスプリッタ 46 と、偏光ビームスプリッタ 46 の合波光入力ポートに接続されたファラデーミラー 47 と、偏光ビームスプリッタ 15、46 の S 偏光出力ポートに両端が接続された位相変調器 17 と、位相変調器 17 を制御する送信側制御手段 20 と、送信側制御手段 20 に接続されて第 1 の乱数を出力する送信側データ処理手段 22 とを備えている。

偏光ビームスプリッタ 15、46、ファラデーミラー 47、位相変調器 17 は、量子通信用の光子パルスに対する両回転方向の光路ループを構成している。

量子送信装置 100 は、量子受信装置 200 から導入された光子パルスを、光ファイバ通信路 1 およびアッテネータ 14 を介してファラデーミラー 47 に導入し、非相対的に偏波面を回転・反射した後、再度アッテネータ 14 および光ファイバ通信路 1 を介して量子受信装置 200 に向けて反射するようになっている。



量子受信装置 200 は、光子発生器 4 と、光子発生器 4 の出力光路に接続されたサーキュレータ 48 と、サーキュレータ 48 の他端に P 偏光出力ポートが接続された偏光ビームスプリッタ 6 と、サーキュレータ 48 のもう一端に接続された光子検出器 19 と、偏光ビームスプリッタ 6 の合波光入力ポートに接続された半波長板 49 と、偏光ビームスプリッタ 6 の S 偏光出力ポートに接続された光子検出器 18 と、半波長板 49 に P 偏光出力ポートが接続された  $2 \times 2$  偏光ビームスプリッタ 50 と、偏光ビームスプリッタ 50 の S 偏光出力ポートと対向するもう 1 つのポートを短絡するループ状光路と、偏光ビームスプリッタ 50 の合波光入力ポートと接続する偏光変調器 51 と、偏光変調器 51 に合波光入力ポートが接続された偏光ビームスプリッタ 11 と、偏光ビームスプリッタ 11 の S 偏光出力ポートに接続された位相変調器 13 と、偏光ビームスプリッタ 11 の P 偏光出力ポートに P 偏光出力ポートが接続され、かつ、位相変調器 13 の他端が S 偏光出力ポートに接続され、かつ、合波光入力ポートが光ファイバ通信路 1 に接続された偏光ビームスプリッタ 12 と、光子検出器 18、19 の検出信号を取り込み、かつ、偏光変調器 51 と位相変調器 13 と光子検出器 18、19 と光子発生器 4 を制御する受信側制御手段 21 と、受信側制御手段 21 に接続されて第 2 の乱数を出力し、光子検出信号を入力する受信側データ処理手段 23 とを備えている。

量子受信装置 200 内の偏光ビームスプリッタ 12 は、光ファイバ通信路 1 を介して量子送信装置 100 内のアッテネータ 14 に接続され、受信側制御手段 21 は、制御信号通信路 3 を介して送信側制御手段 20 に接続され、受信側データ処理手段 23 は、公開通信路 2 を介して送信側データ処理手段 22 に接続されている。

量子受信装置 200 内において、偏光ビームスプリッタ 50 から 2 連光子パルスが偏光変調器 51 に向かって出力されるが、先行する参照光パルスは P 偏光の偏波面を持っているのに対し、後続する信号光パルスは S 偏光の偏波面を持っている。このため、偏光変調器 51 が通過する信号光パルスのみ偏波面を直角に回転し、量子受信装置 200 から量子送信装置 100 へ伝送する際には、2 連光子パルスを P 偏光に偏波面を揃えて、偏光ビームスプリッタ 11、12 を透過させる。

S 偏光した 2 連光子パルスが量子送信装置 100 から量子受信装置 200 へ帰還した際には、偏光ビームスプリッタ 12 で反射され位相変調器 13 を経由する光路が選択される。位相変調器 13 を通過した 2 連光子パルスは、偏光ビームスプリッタ 11 で反射され、偏光変調器 51 を通過する、2 連光子パルスが偏光変調器 51 を通過する際、偏光変調器 51 は、信号光パルスのみ偏波面を直角に回転し、P 偏光の偏波面にする。このため、偏光ビームスプリッタ 50 で参照光パルスは完全に反射されてループ状光路を経た後、半波長板 49 に向かい、信号光パルスは、偏光ビームスプリッタ 50 を透過し半波長板 49 に直行することになる。

次に、図 5 に示したこの発明の実施の形態 2 に係る量子暗号通信装置の動作について説明する。

受信側制御手段 21 は、制御信号通信路 3 を介した制御信号の相互通信により、量子送信装置 100 内の送信側制御手段 20 と同期・調歩動作する。量子受信装置 200 内の光子発生器 4 は、受信側制御手段 21 が出力する同期信号に応じて、偏波面の揃った光子パルスを発生する。

光子発生器 4 から発生した光子パルスは、サーキュレータ 48 を経て偏光ビームスプリッタ 6 に入光する。なお、光子パルスは偏光ビームスプリッタ 6 の P 偏光に偏波面が揃っているとする。

光子パルスは、偏光ビームスプリッタ 6 を透過し、半波長板 49 に導かれる。

半波長板 49 によって、偏波面が 45 度回転させられた後、偏光ビームスプリッタ 50 に入光する。光子パルスは偏波面が 45 度傾いているため、P 偏光である参照光パルスと S 偏光である信号光パルスの 2 つの光子パルスに分離される。信号光パルスは、ループ状光路を経た後、偏光ビームスプリッタ 50 の偏光変調器 51 に接続する合波光出力ポートから出力され、先行する参照光パルスと後続する信号光パルスからなる 2 連光子パルスが偏光変調器 51 に導かれる。

偏光変調器 51 に導かれた 2 連光子パルスのうち、S 偏光である信号光パルスは偏光変調器 51 により偏波面を直角に回転させられ、P 偏光になる、このため、偏光変調器 51 を通過後、偏光ビームスプリッタ 11 に導かれた 2 連光子パルスは、偏光ビームスプリッタ 11、12 をこの順に通過し、位相変調器 13 のあ

る迂回光路に導かれることなく、光ファイバ通信路 1 に導かれる。

- 5     なお、図 5 における量子受信装置 200 の光学系の構成例としては種々採用できる。図 6 A は、図 5 に示す量子受信装置 200 において、1 つの光子パルスから 2 連光子パルスに分離・出力するための光学系の構成例であり、1×2 偏光ビームスプリッタ 6 と、半波長板 49 と、2×2 偏光ビームスプリッタ 50 と、ループ状光路を用い、位相変調器用迂回光路の構成例として、偏光変調器 51 と、1×2 タイプの偏光ビームスプリッタ 11、12 との 2 個を用いた構成例を示したが、図 6 B に示すように、1×2 タイプの偏光ビームスプリッタ 52、53 の 2 式用いた 2 連光子パルス分離・出力光学系の構成例や、図 6 C に示すように、10     2×2 偏光ビームスプリッタ 54 を 1 式用いた迂回光路の構成例や、図 6 D に示すように、ビームスプリッタ 55 と、偏光コントローラ 56 と、ミラー 57、58 と、偏光ビームスプリッタ 59 を用いた 2 連光子パルス分離・出力光学系の構成例や、図 6 E に示すように、カプラ 60 と、遅延ファイバ 61 と、偏光コントローラ 62 と、偏光ビームスプリッタ 63 とを用いた 2 連光子パルス分離・出力  
15     光学系の構成例も存在し、特定の 1 つの構成例に特化されるものではない。

量子受信装置 200 から光ファイバ通信路 1 に導かれた 2 連光子パルスは、量子送信装置 100 に導入され、量子送信装置 100 内のファラデーミラー 47 により偏波面を非相反的に直角に回転・反射させられ、位相変調器 17 により信号光パルスが位相変調を受けた後、再び量子受信装置 200 に帰還してくる。

- 20     なお、図 5 においては、量子送信装置 100 の光学系の構成例として、アッテネータ 14 と、偏光ビームスプリッタ 15、46 と、ファラデーミラー 47 と、位相変調器 17 を用いた構成例を示したが、実施の形態 1 と同様に、図 3 A - 図 3 E に示したような構成例も存在し、特定の 1 つの構成例に特化されるものではない。

- 25     量子受信装置 200 に帰還した 2 連光子パルスは、偏光ビームスプリッタ 12 で完全に反射されて、位相変調器 13 が配置された迂回光路に導かれる。なぜならば、光ファイバ通信路 1 の一方の端点で入射された光は、他方の端点で非相反的に直角に偏波面の回転を受けて反射して帰還する場合に、途中の光路でいかなる複屈折性の揺らぎが存在したとしても、入射した時点から直角に偏波面が回転

した状態で帰還するからである。

偏光ビームスプリッタ 1 2 で反射された 2 連光子パルスは、位相変調器 1 3 に入光する。このとき、位相変調器 1 3 は、受信側制御手段 2 1 の制御下で、受信側データ処理手段 2 3 が出力した第 2 の乱数に応じて、参照光パルスのみに対して位相変調をかける。

位相変調器 1 3 を通過した 2 連光子パルスは、偏光ビームスプリッタ 1 1 で完全に反射されて偏光変調器 5 1 へと導かれる。2 連光子パルスが偏光変調器 5 1 を通過する際、信号光パルスのみ偏波面を直角に回転させられ、S 偏光から P 偏光にかわる。

10 偏光変調器 5 1 を通過した 2 連光子パルスは、偏光ビームスプリッタ 5 0 に導入される。S 偏光である参照光パルスは、偏光ビームスプリッタ 5 0 において完全に反射させられて、ループ状光路を経た後、半波長板 4 9 に導かれる。一方、P 偏光である信号光パルスは、偏光ビームスプリッタ 5 0 を透過し、半波長板 4 9 に導かれる。

15 このとき、参照光パルスは、信号光パルスが量子受信装置 2 0 0 から量子送信装置 1 0 0 に向かう往路で通過したときと同一のループ状光路を通過するので、参照光パルスと信号光パルスの間の時間差は完全に打ち消されて、1 つの光子パルスとして合流・干渉を引き起こすことになる。干渉を引き起こした光子パルスは、この干渉の場合は、偏波面が排他的に 2 つの直交する偏波面のいずれか 1 つ

20 となる。

半波長板 4 9 に導かれた、干渉を引き起こした光子パルスは、半波長板 4 9 により偏波面を -45 度回転させられた後、偏光ビームスプリッタ 6 に導かれる。偏光ビームスプリッタ 6 に導かれた光子パルスは、干渉の結果、排他的に 1 対の光子検出器 1 8、1 9 のいずれかに接続する一方のポートに導かれ、一方の光子

25 検出器を発火する。なお、光子検出器 1 9 に接続するポートに導かれた光子パルスは、サーキュレータ 4 8 により光子検出器 1 9 に導かれることになる。

受信側制御手段 2 1 は、光子検出器 1 8、1 9 のいずれが発火したかをビット情報に変換し、受信側データ処理手段 2 3 に伝送する。

受信側データ処理手段 2 3 は、第 2 の乱数と、量子情報で伝送されたビット情

報とから、公開通信路 2 を用いて、量子送信装置 100 と情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

次に、量子送信装置 100 に注目しながら、具体的な動作について説明する。

量子受信装置 200 から光ファイバ通信路 1 を通過して量子送信装置 100 に  
5 導入された 2 連光子パルスは、量子送信装置 100 に到達した時点では、光ファイバ通信路 1 の有する複屈折性の揺らぎにより偏波面が完全にランダムな状態になっている。

この状態で、量子送信装置 100 に導入された 2 連光子パルスは、アッテネータ 14 で減衰された後、偏光ビームスプリッタ 15 によりそれぞれ直交する 2 つ  
10 の偏波モード（P 偏光と S 偏光）に分離される。

このようにして、4 つに分離された光子パルスのうち、時計回りに進行する 2 連光子パルス（S 偏光）は、偏光ビームスプリッタ 15 で反射され、位相変調器 17 を通過した後、偏光ビームスプリッタ 46 で反射され、ファラデーミラー 47 に導かれる。ファラデーミラー 47 で非相対的に偏波面を直角に回転・反  
15 射させられた後、偏光ビームスプリッタ 46 を透過し、偏光ビームスプリッタ 15 に戻る。

また、4 つに分離された光子パルスのうち、反時計回りに進行する 2 連光子パルス（P 偏光）は、偏光ビームスプリッタ 15、46 を通過し、ファラデーミラー 47 で非相対的に偏波面を直角に回転・反射させられ、偏光ビームスプリッタ 46 で反射され、位相変調器 17 を通過した後、偏光ビームスプリッタ 15 に  
20 戻る。

このとき、位相変調器 17 は、送信側制御手段 20 の制御下で、送信側制御手段 22 が出力した第 1 の乱数に応じて、2 連光子パルスのうち信号光パルスのみに対して、時計回りまたは反時計回りの進行方向に依存することなく、位相変調器 17 を通過する際に位相変調をかけている。  
25

偏光ビームスプリッタ 15 に戻った 4 つの光子パルスは、分離合流するまでの光路長が、時計回りまたは反時計回りに依存せずに等しいので、再び 2 連光子パルスとなり、アッテネータ 14 に導入される。ここで、アッテネータ 14 の光子レベル強度の減衰の大きさは、信号光パルスの光子数が「1」を越えない強度と

なるように調整されている。

このようにして、再び光ファイバ通信路 1 に導入されて量子受信装置 200 に  
帰還した 2 連光子パルスは、前述したとおり、偏光ビームスプリッタ 12 により  
完全に反射されて、位相変調器 13 のある迂回光路を通った後、偏光ビームスプ  
5 リッタ 11 で反射されて、光子検出器 18、19 の設置されたポートに導かれる

以下、受信側制御手段 21 は、光子検出器 18、19 のいずれが発火したかを  
ビット情報に変換して受信側データ処理手段 23 に伝送する。

上記の 1 パルス当たりの量子通信を、あらかじめ定めた回数だけ繰り返した後  
10 、送信側データ処理手段 22 および受信側データ処理手段 23 は、量子伝送路（  
光ファイバ通信路 1）を介して秘匿性を保って伝送された情報と、公開通信路 2  
を介して伝送された情報とを用いて秘匿性情報を共有する。すなわち、第 1 およ  
び第 2 の乱数と、量子通信で伝送されたビット情報とから、公開通信路 2 を用い  
て、情報の一部を交換しつつ、秘匿性が保証されたランダムな情報を共有する。

15 次に、図 7 に示すフローチャートを参照しながら、図 5 に示したこの発明の実  
施の形態 2 による量子通信動作について、さらに具体的に説明する。

図 7 において、量子暗号通信装置の光子パルス（量子暗号）に関連した量子通  
信部の処理ステップは、光子発生ステップ S1 と、光パルス分離・合流ステップ  
S2 と、信号光パルスの偏波面を回転させる第 1 偏波回転ステップ S3 と、位相  
20 変調器 13 のない光路を選択する光路選択ステップ S4 と、量子受信装置 200  
から量子送信装置 100 への量子通信用の光子供給（往路）ステップ S5 と、送  
信側での第 1 アッテネートステップ S6 と、第 1 ファラデー回転反射ステップ  
S7 と、第 1 送信側位相変調ステップ S8 と、第 2 送信側位相変調ステップ S7  
a と、第 2 ファラデー回転反射ステップ S8 a と、第 2 アッテネートステップ  
25 S9 と、量子送信装置 100 から量子受信装置 200 への量子通信用の光子伝送  
（復路）ステップ S10 と、受信側位相変調ステップ S11 と、再び信号光パル  
スの偏波面を回転させる第 2 偏波回転ステップ S12 と、光子分離・合流・干渉  
ステップ S13 と、光子検出ステップ S14 とを含む。

まず、量子受信装置 200 内の光子発生器 4 は、受信側制御手段 21 の制御下

で光子パルスが発生する。発生した光子パルスは、サーキュレータ 48 により偏光ビームスプリッタ 6 に導かれる。光子パルスは、P 偏光に偏波面が揃えられている（光子発生ステップ S 1）。なお、光子パルスは、例えばレーザーパルスのように、パルス当たりの光子数がポアソン分布に従うように発生されてもよく、

- 5 単一光子源を用いて、パルス当たり単一光子として発生されてもよい。

偏光ビームスプリッタ 6 に導かれた光子パルスは、偏光ビームスプリッタ 6 を透過し、半波長板 49 に導かれ、偏波面を 45 度回転させられる。偏波面を 45 度回転させられた光子パルスは、偏光ビームスプリッタ 50 に導かれ、P 偏光である参照光パルスと S 偏光である信号光パルスに分離される。信号光パルスは、

- 10 ループ上光路を経た後、参照光パルスと合流して、2 連光子パルスとして偏光変調器 51 に向かって出力される（光パルス分離・合流ステップ S 2）。

偏光変調器 51 に導かれた 2 連光子パルスは、信号光パルスのみ偏波面を直角に回転させられて、偏波面の揃った 2 連光子パルスとなる（第 1 偏波回転ステップ S 3）。

- 15 偏光変調器 51 から出力された 2 連光子パルスは、参照光パルスと信号光パルスのいずれの光子パルスも偏波面が偏光ビームスプリッタ 11、12 に対して P 偏光となるように偏波面が揃っているので、偏光ビームスプリッタ 11 および 12 を透過する光路が選択される（光路選択ステップ S 4）。

- 20 偏光ビームスプリッタ 12 を透過した 2 連光子パルスは、光ファイバ通信路 1 に導かれ、そのまま量子送信装置 100 に伝送される（光子供給（往路）ステップ S 5）。このとき、光ファイバ通信路 1 が有する複屈折性の揺らぎにより、2 連光子パルスの偏波面は完全にランダムな状態になってしまう。

- 25 量子送信装置 100 に導かれた 2 連光子パルスは、アッテネータ 14 を透過することによって、パルス当たりの光子数が減衰された後、偏光ビームスプリッタ 15 に導かれる（第 1 アッテネートステップ S 6）。

また、量子送信装置 100 に導入された 2 連光子パルスは、各偏波面がランダムなので、偏光ビームスプリッタ 15 において、時計回りで周回する光子パルスと反時計回りで周回する光子パルスとに分離された後、再び偏光ビームスプリッタ 46 で合流して 2 連光子パルスに戻る。

すなわち、2連光子パルスの中の反時計回りの光子パルスは、光路ループ内において、偏光ビームスプリッタ46、ファラデーミラー47、偏光ビームスプリッタ46および位相変調器17の順に通過し、ファラデーミラー47を通るときに、偏波面が非相対的に直角に回転・反射させられる（第1ファラデー回転反射ステップS7）。

また、反時計回りの光子パルスは、ファラデーミラー47で反射された後、位相変調器17に導入され、位相変調器17を通過する際に、信号光パルスに当たる光子パルスのみが位相変調を受ける（第1送信側位相変調ステップS8）。

このときの位相変調の大きさは、送信側制御手段20により制御され、送信側データ処理手段22が出力した第1の乱数に応じて、制御信号通信路3を介して、同期タイミングを調整しつつ位相変調をかけることによって決定される。

一方、量子送信装置100に導入された2連光子パルスのうち、時計回りの光子パルスの場合は、光路ループ内において、位相変調器17およびファラデーミラー47の順に通過するので、先に第2送信側位相変調ステップS7aを経た後に、第2ファラデー回転反射ステップS8aが実行される。なお、ファラデーミラー（非相反素子）47による非相対的な偏波面の回転とは、回転の向きが光子パルスの進行方向に依存しないことを意味する。

また、光路ループ内の位相変調器17において、反時計回りの光子パルスおよび時計回りの光子パルスのいずれに対しても、信号光パルスのみに対して選択的に位相変調をかけるためには、偏光ビームスプリッタ15、46、ファラデーミラー47および位相変調器17を含む光路ループの光路長を、入射される2連光子パルスの時間差に相当する距離に比べて十分に短く設定すればよく、容易に実現することができる。

偏光ビームスプリッタ15を介して、再び2連光子パルスに戻った光子パルスは、アッテネータ14を再度通過する。このとき、信号光パルスの光子数が「1」を越えない程度まで、パルス当たりの光子レベル強度が減衰された後、光ファイバ通信路1に導入される（第2アッテネートステップS9）。

光ファイバ通信路1に再入射した2連光子パルスは、量子受信装置200に向かって帰還することになるが、このとき、2連光子パルスの偏波状態は、光ファ



イバ通信路 1 の有する複屈折性の揺らぎによって、再びランダムな変動を受ける

。

- しかし、光ファイバ通信路 1 に再入射した 2 連光子パルスの偏波面は、量子送信装置 100 内のファラデーミラー 47 により、非相反的に直角に回転を受けているので、光ファイバ通信路 1 の往路上で受けた偏波変動と、復路上で受けた偏波変動が丁度打ち消し合うように作用する。

- 従って、再導入された 2 連光子パルスが量子受信装置 200 内の偏光ビームスプリッタ 12 に到達する時点では、2 連光子パルスの偏波面は、偏光ビームスプリッタ 12 から量子送信装置 100 に向かった往路時と比べて、正確に直角に回転している（光子伝送（復路）ステップ S10）。

- このように、量子受信装置 200 に到達した 2 連光子パルスは、偏波面が直角に回転した、偏光ビームスプリッタ 12 にとって S 偏光にあたる偏波面でもって、偏光ビームスプリッタ 12 に導かれるので、偏光ビームスプリッタ 12 において完全に反射され、位相変調器 13 のある迂回光路に導かれる。2 連光子パルスが位相変調器 13 を通過する際に、参照光パルスのみが位相変調を受ける（受信側位相変調ステップ S11）。このときの位相変調の大きさは、受信側制御手段 21 により制御され、受信側データ処理手段 23 が出力した第 2 の乱数に応じて、位相変調の大きさが決定される。

- 2 連光子パルスは、位相変調器 13 を通過後、偏光ビームスプリッタ 11 で完全に反射されて、偏光変調器 51 に導かれる。

偏光変調器 51 に導入された 2 連光子パルスは、偏光変調器 51 を通過する際、信号光パルスのみ偏波面を直角に回転させられ、S 偏光から P 偏光となる（第 2 偏波回転ステップ S12）。

- 偏光変調器 51 から偏光ビームスプリッタ 50 に導かれた 2 連光子パルスは、参照光パルスが偏光ビームスプリッタ 50 で完全に反射され、ループ状光路を通る。信号光パルスは偏光ビームスプリッタ 50 を透過する。従って、偏光ビームスプリッタ 50 から出力される際、参照光パルスと信号光パルスは同時に出力され、合流して 1 つの光子パルスとなる。参照光パルスと信号光パルスが合流する際、干渉が引き起こされる。干渉の結果、偏波面が排他的に 2 つの直交する偏波

面のいずれか1つとなっている。

- 干渉を引き起こした光子パルスは、半波長板49に導かれ、偏波面を-45度回転させられる。偏波面を-45度回転させられた干渉を引き起こした光子パルスは、偏波ビームスプリッタ6に導かれ、光子検出器18、19のあるいずれか一方のポートへ出力される（光子分離・合流・干渉ステップS13）。干渉を引き起こした光子パルスは、光子検出器18または19のいずれかの一方に排他的に導かれることになる。

なお、光子検出器19のある光路に導かれた光子パルスは、サーキュレータ48により光子検出器19に導かれる。

- 干渉を引き起こした光子パルスが光子検出器18、19のどちらかに導かれるかは、第1送信側位相変調ステップS8において信号光パルスが受けた位相変調と、受信側位相変調ステップS11において参照光パルスが受けた位相変調との位相差により確率的に決定される。但し、上記位相差が「0」または「 $\pi$ 」の場合には、干渉を引き起こした光子パルスの導かれる光子検出器が確定する。
- 受信側制御手段21は、光子検出器18、19のどちらかが発火したことにより、「0」または「1」の量子通信ビット情報を定め、この量子通信ビット情報を受信側データ処理手段23に送る（光子検出ステップS14）。

以上が量子通信部の光子パルス当たりの動作フローである。

- 上記量子通信動作は、予め定めた回数だけ繰り返し実行され、その後、送信側データ処理手段22および受信側データ処理手段23は、公開通信路2を用いて相互に情報交換をしつつ、第1および第2の乱数と量子通信ビット情報から、秘匿性が保証されたランダムな情報を共有する。

- このように、量子受信装置200から出力されて、量子受信装置200に再び導入される光子パルスは、光ファイバ通信路1の有する任意の複屈折性揺らぎに起因してランダムな偏波変動が生じても、光ファイバ通信路1の送信側端（量子送信装置100内のファラデーミラー47）で非相反的に直角に偏波面が回転・反射されて往復することにより、ランダムな偏波変動が打ち消されることになる。

従って、量子受信装置200に再導入された光子パルスは、偏波面が自動的に

完全に整えられているので、偏波無依存性が要求されることは全くなく、偏波依存性を有していたとしても、光子パルスの偏波面の調整が全く不要となる。

また、往路において光子パルスを2連光子パルスに分離するために用いた光学系と、復路において、2連光子パルスを合流・干渉させるために用いた光学系に  
5 同一のものをを用いているため、光路長差の調整が全く不要であり、かつ、光路長揺らぎに対しても自動的に補償されるような構成となり、安定な干渉系を構成することができる。

また、量子受信装置200内の光路において、2連光子パルスの偏波面が揃っていない場合でも、一方の光子パルスのみに選択的に偏光変調をかけ偏波面を揃  
10 えること、位相変調器13を通る迂回光路を設け、上記のような量子送信装置100内で偏波面が直角に回転されることを利用して、量子受信装置200内で、光子発生器4から光ファイバ通信路1に向かう往路においては、光子パルスが位相変調器13の無い光路を自動的に選択し、光ファイバ通信路1から光子検出器18、19に向かう復路においては、光子パルスが位相変調器13のある迂回光  
15 路を自動的に選択するようにしたことで、位相変調器13において光子パルスの流れは一方向に限定され、光子パルスに不適切な位相変調がかけられるおそれが全くなくなり、光子パルス発生の繰り返し周波数を自由に選択することができる。

## 20 産業上の利用の可能性

以上のように、この発明によれば、偏波面制御は不要で、光路長揺らぎに安定し、かつ動作周波数が自由に選択できる量子暗号通信装置を実現できる。

## 請 求 の 範 囲

1. 量子を伝送するための量子通信路と、  
前記量子伝送路の送信側に設置された量子送信装置と、
- 5 前記量子伝送路の受信側に設置された量子受信装置と、  
前記量子送信装置と前記量子受信装置を結合して同期信号を含む制御信号を相互通信するための制御信号通信路と  
を備えた量子暗号通信装置であって、  
前記量子受信装置は、
- 10 量子源となる光源と、  
前記光源から出た光子パルスから信号光パルスと参照光パルスとの時間差 2 連光子パルスを発生すると共に、逆進する量子である信号光パルスと参照光パルスとを合波、干渉させるための合波干渉手段を有するループ状光路と、  
前記量子通信路との接続口に設けられて、前記時間差 2 連光子パルスが前記
- 15 量子通信路を介して前記量子送信装置と前記量子受信装置との間を往復した後、  
受信される前記参照光パルスのみに対して位相変調をかける位相変調器を有する迂回光路と、  
前記ループ状光路を介した干渉光を観測する光子検出器と  
を含み、
- 20 前記量子送信装置は、  
前記量子受信装置から前記量子通信路を介して到達した 2 連光子パルスの偏波面を非相反的に直角に回転させる偏波回転手段と、  
前記偏波回転手段を通過した信号光パルスに位相変調をかけて再び量子通信路を通過して前記量子受信装置に戻す位相変調器と、
- 25 信号光パルスをパルス中に光子が 2 個以上含まない状態まで減光する減光手段と  
を含む  
ことを特徴とする量子暗号通信装置。

2. 請求項1記載の量子暗号通信装置において、  
前記迂回光路の送信光路と受信光路との分岐点に、前記2連光子パルスの前記信号光パルスと前記参照光パルスの偏波面が同じ場合、帰還光子パルスのみ前記位相変調器のある受信光路を通過させる偏光ビームスプリッタを設けた
- 5 ことを特徴とする量子暗号通信装置。
3. 請求項1記載の量子暗号通信装置において、  
前記ループ状光路と前記迂回光路との間に、前記2連光子パルスの信号光パルスと参照光パルスの偏波面が異なる場合、信号光パルスが通過するときのみ偏波面を回転することで、往路での2連光子パルスの偏波面を揃える偏光変調器を設けた
- 10 ことを特徴とする量子暗号通信装置。
4. 請求項2または3に記載の量子暗号通信装置において、
- 15 前記偏光ビームスプリッタとして、 $1 \times 2$ 入出力型偏光ビームスプリッタを2式用い、特定の偏波面の光子パルスのみを前記位相変調器のある受信光路に導くことを特徴とする量子暗号通信装置。
5. 請求項2または3に記載の量子暗号通信装置において、
- 20 前記偏光ビームスプリッタとして、 $2 \times 2$ 入出力型偏光ビームスプリッタを1式用い、特定の偏波面の光子パルスのみを位相変調器のある受信光路に導くことを特徴とする量子暗号通信装置。

図 1

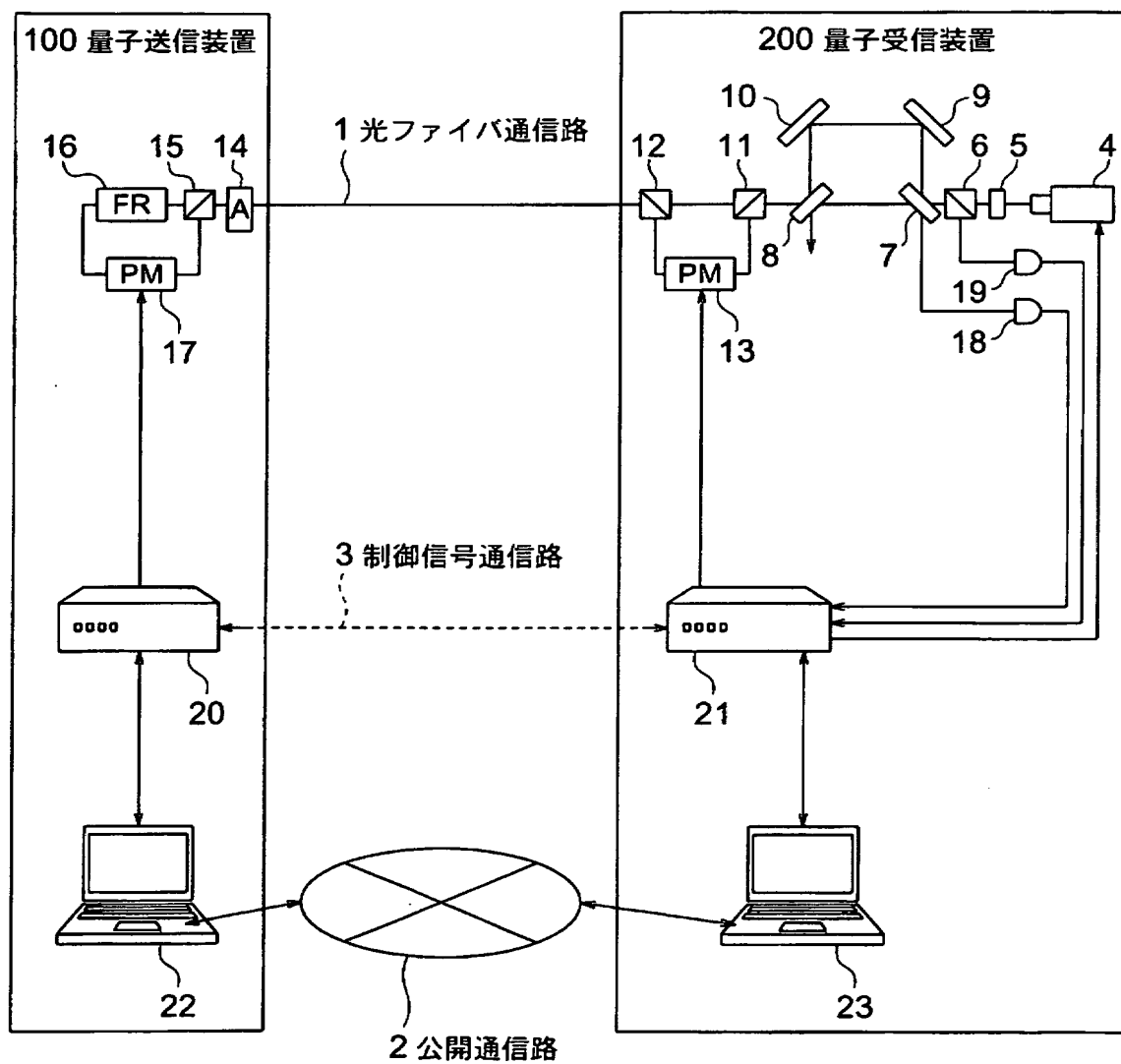


図 2A

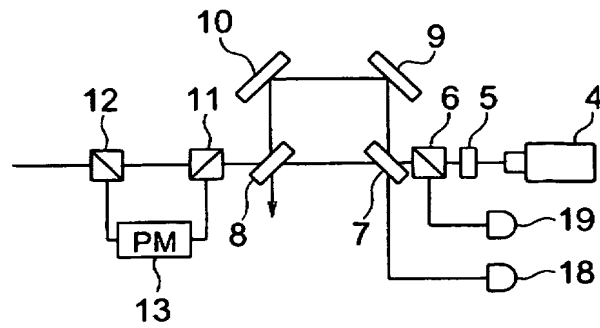


図 2B

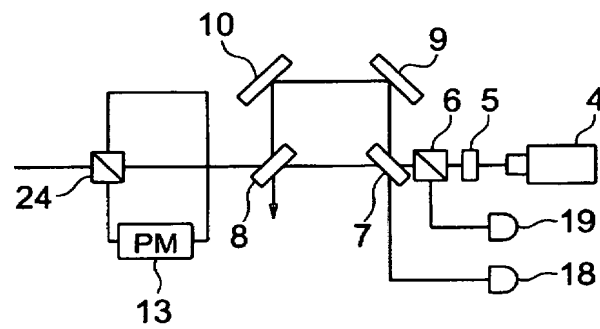


図 2C

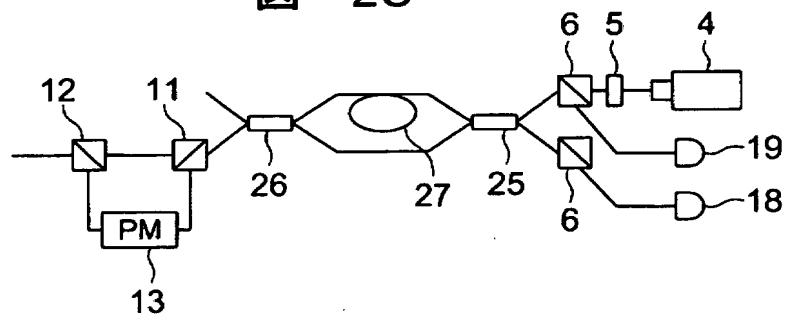


図 2D

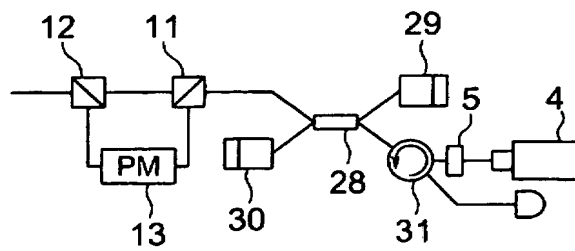






図 4

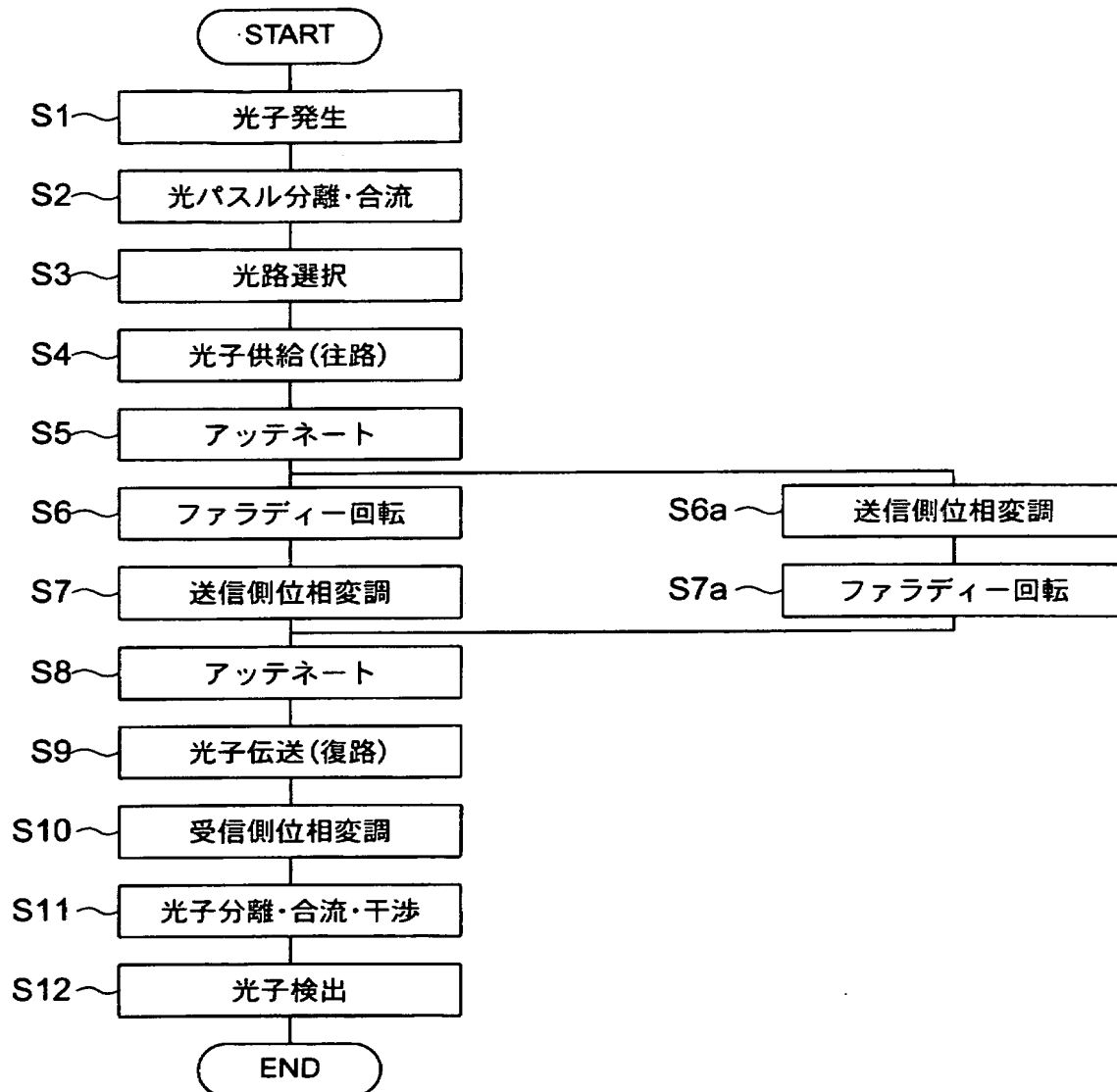


図 5

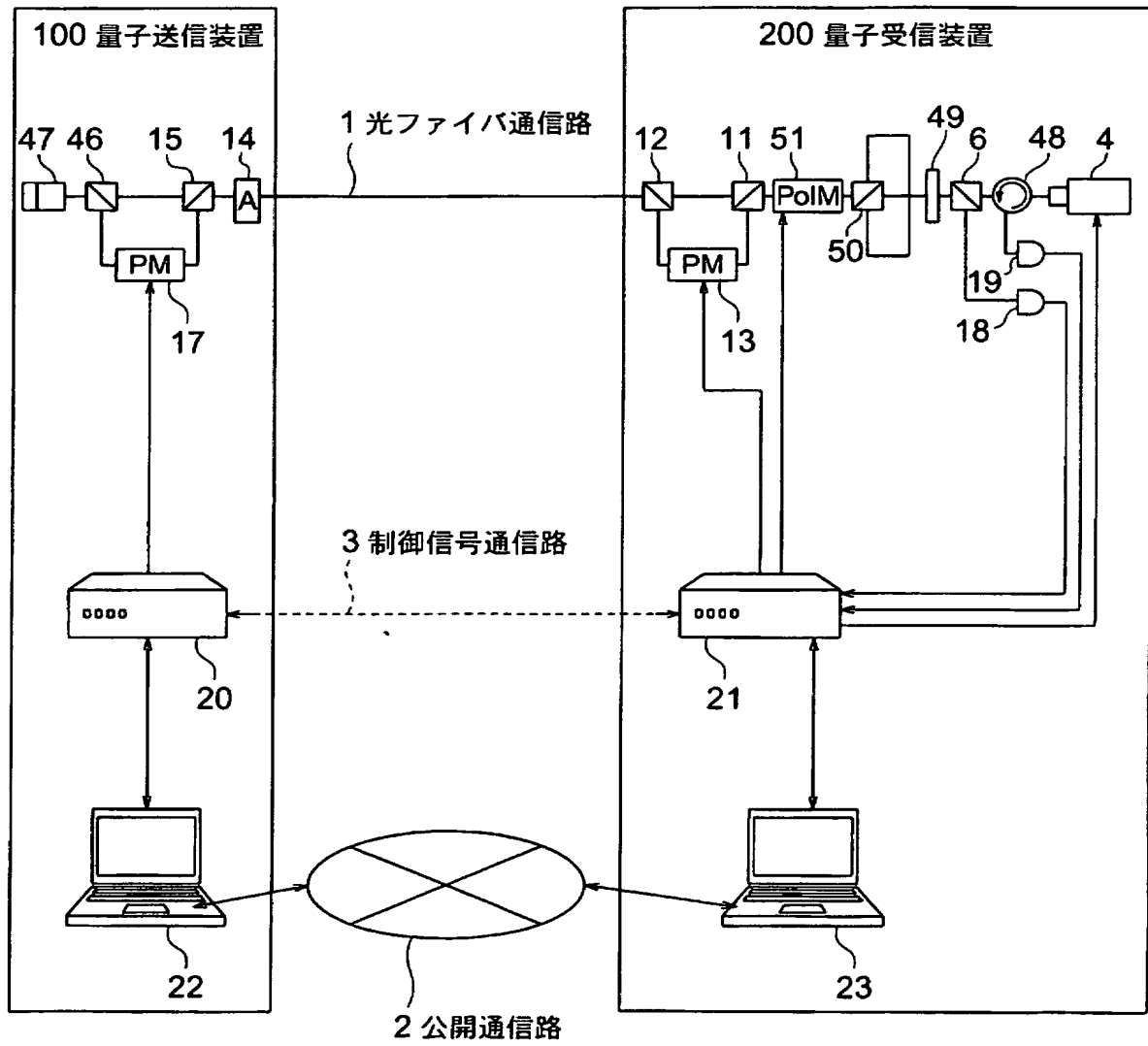


図 6A

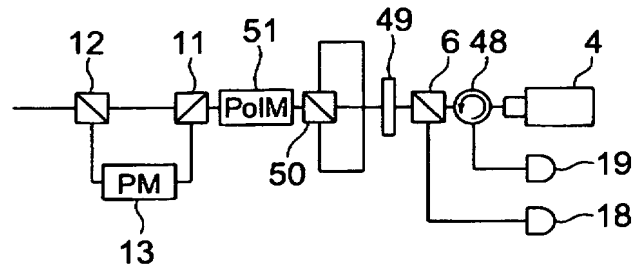


図 6B

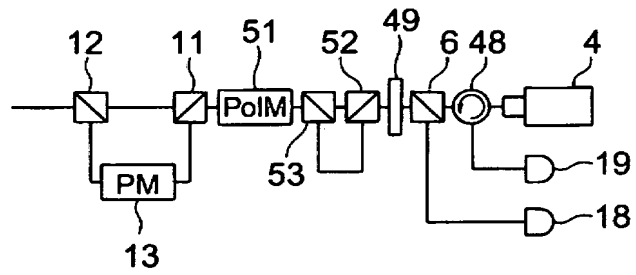


図 6C

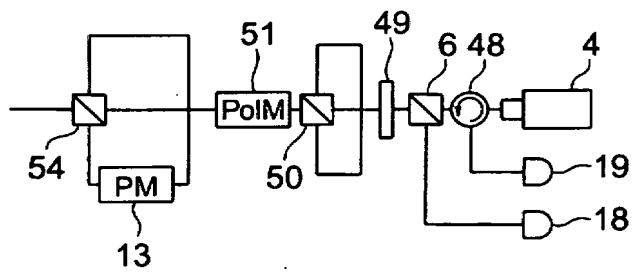


図 6D

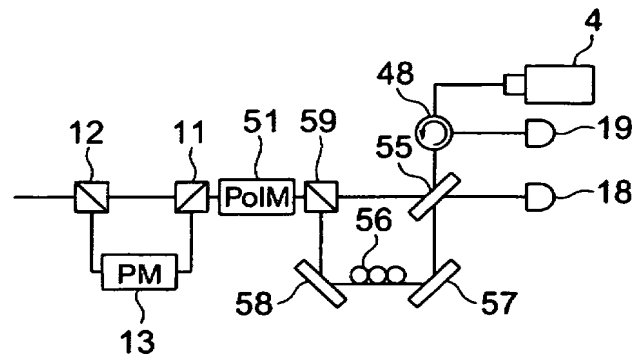


図 6E

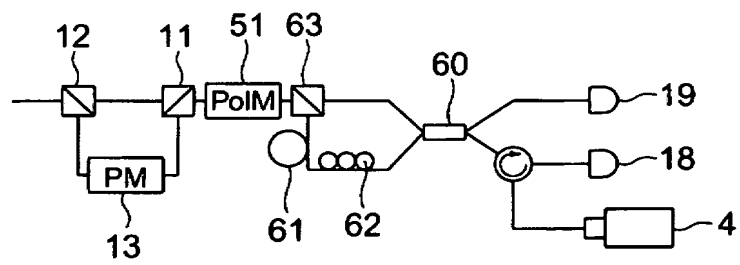
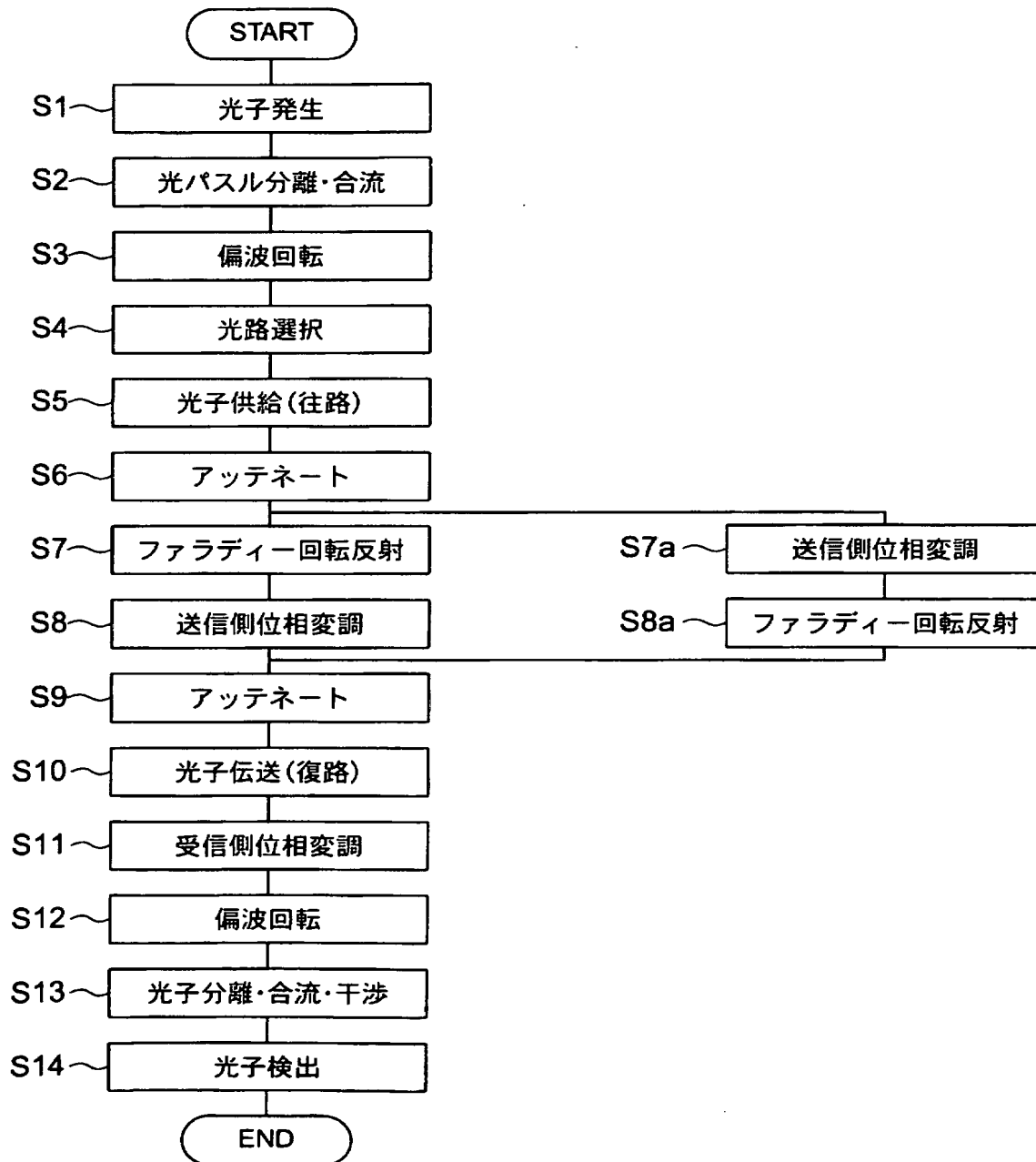


図 7



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007001

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L9/12, H04B10/00, G02F1/01

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L9/12, H04B10/00, G02F1/01

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS), WPI, INSPEC (DIALOG)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Toshio HASEGAWA, Jun'ichi ABE: "Kanryugata Ryoshikagi Haifu", 2002 Nen Ango to Joho Security Symposium Yokoshu, 29 January, 2002 (29.01.02), Volume 1 of 2, pages 43 to 48	1-5
Y	Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Toshio HASEGAWA and Jun'ichi ABE: "'Circular Type' Quantum Key Distribution", IEEE PHOTONICS TECHNOLOGY LETTERS, receive on 19 April, 2002 (19.04.02), Vol.14, No.4, pages 576 to 578	1-5

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
03 August, 2004 (03.08.04)Date of mailing of the international search report  
24 August, 2004 (24.08.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007001

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Mitsuru MATSUI, Shigeki TAKEUCHI: "Chokyoru Ryoshi Ango Tsushin System Jikken", 2003 Nen Ango to Joho Security Symposium Yokoshu, 26 January, 2003 (26.01.03), Volume 2 of 2, pages 1125 to 1130	1-5
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Katsuhiro SHIMIZU, Mitsuru MATSUI and Shigeki TAKEUCHI: "An Experimental Realization of Quantum Cryptosystem", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E85-A, No.1, 01 January, 2002 (01.01.02), pages 149 to 157	1-5

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl. H04L9/12, H04B10/00, G02F1/01		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl. H04L9/12, H04B10/00, G02F1/01		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国登録実用新案公報 1994-2004年 日本国実用新案登録公報 1996-2004年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
JICSTファイル (JOIS), WPI, INSPEC (DIALOG)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	西岡毅, 石塚裕一, 長谷川俊夫, 安部淳一: "環流型量子鍵配布" 2002年暗号と情報セキュリティシンポジウム予稿集, 2002. 01. 29, Volume 1 of 2, p. 43-48	1-5
Y	Tsuyoshi Nishioka, Hirokazu Ishizuka, Toshio Hasegawa and Jun'ichi Abe: "Circular Type" Quantum Key Distribution IEEE PHOTONICS TECHNOLOGY LETTERS, 2002. 04. 19受入, VOL14, NO. 4, p. 576-578	1-5
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	03. 08. 2004	国際調査報告の発送日
		24. 8. 2004
国際調査機関の名称及びあて先	特許庁審査官 (権限のある職員)	5M 4229
日本国特許庁 (ISA/JP)	青木 重徳	
郵便番号 100-8915	電話番号 03-3581-1101	内線 3597
東京都千代田区霞が関三丁目4番3号		



C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	長谷川俊夫, 西岡毅, 石塚裕一, 安部淳一, 松井充, 竹内繁樹: “長距離量子暗号通信システム実験” 2003年暗号と情報セキュリティシンポジウム予稿集, 2003. 01. 26, Volume 2 of 2, p. 1125-1130	1-5
Y	Toshio HASEGAWA, Tsuyoshi NISHIOKA, Hirokazu ISHIZUKA, Jun'ichi ABE, Katsuhiro SHIMIZU, Mitsuru MATSUI and Shigeki TAKEUCHI: “An Experimental Realization of Quantum Cryptosystem”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, VOL. E85-A, NO. 1, 2002. 01. 01, p. 149-157	1-5